"Command Risk Managment - Making It Work"

Agenda

Introduction

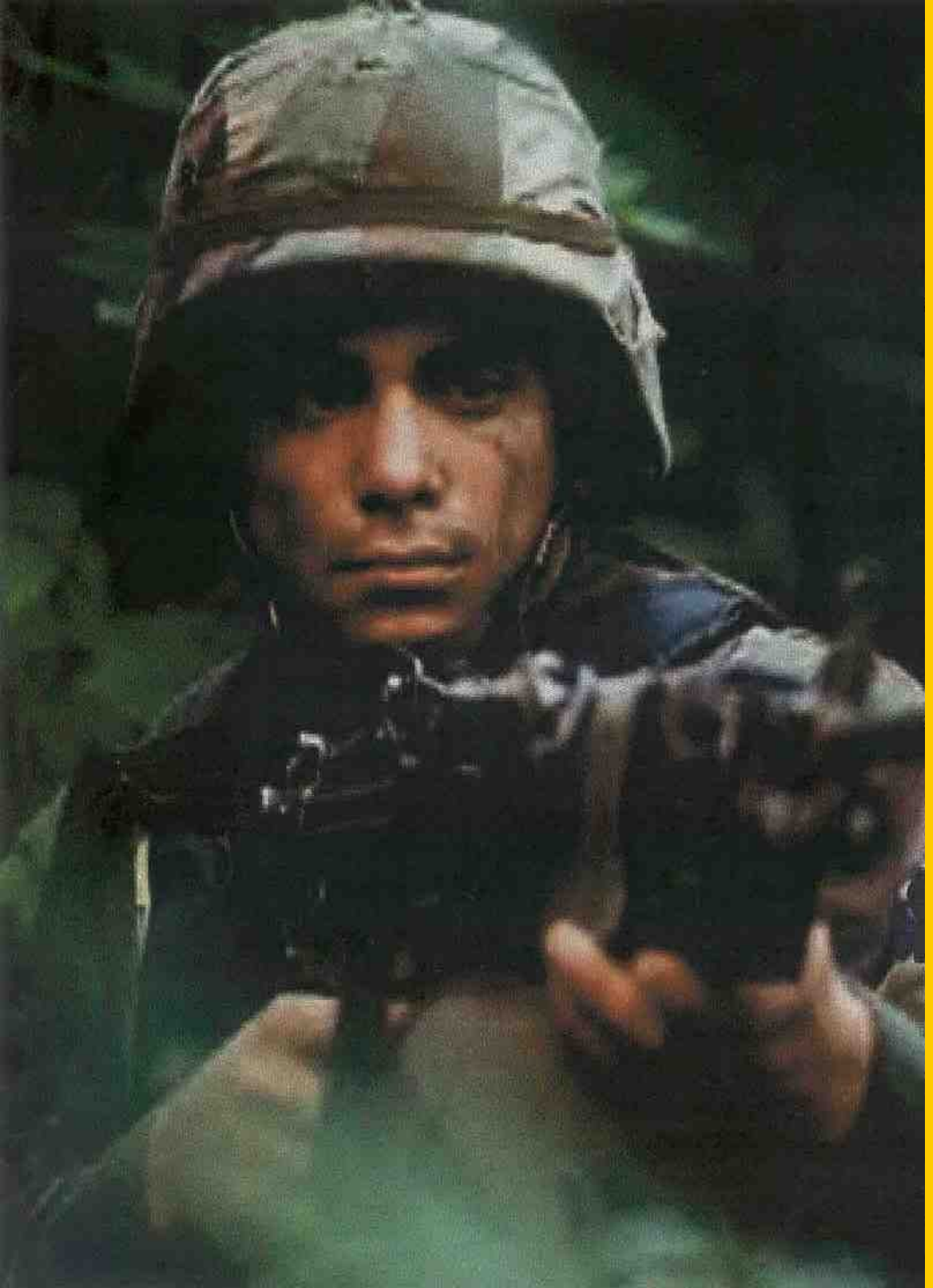
Risk Management

Enterprise Risk Management [ERM]

Current Risk Management Tools

Future Risk Management Tools

Introduction



“First is the Soldier. Our Soldiers are paramount. They will remain the centerpiece of our thinking, our systems, and our combat formations. We must always remember, ‘Humans are more important than hardware’. We must always remember that Soldiers ARE the Army.“

- Peter J. Schoomaker, CSA
AUSA 2003
Washington, DC

Soldier's Creed

I am an American Soldier.

I am a Warrior and a member of a team. I serve the people of the United States and live the Army Values.

I will always place the mission first.

I will never accept defeat.

I will never quit.

I will never leave a fallen comrade.

I am disciplined, physically and mentally tough, trained and proficient in my warrior tasks and drills. I always maintain my arms, my equipment and myself.

I am an expert and I am a professional.

I stand ready to deploy, engage, and destroy the enemies of the United States of America in close combat.

I am a guardian of freedom and the American way of life.

I am an American Soldier.

WARRIOR ETHOS

To be a leader today…

" …to be a manager in the modern world is to take responsibility for controlling what is less and less controllable…today's executives must be leaders… in permanent white water"

- Peter Vaill, 1989

A New Kind of Leader

“We need to build into the system thinkers who dare to ask the question no one else considered or dared to ask.”

General (Ret.) Montgomery C. Meigs
in *Unorthodox Thoughts about Asymmetric Warfare*

"You see things as they are and ask, 'Why?' I dream things as they never were and ask, 'Why not?'

George Bernard Shaw

Cultural Change: The To-Do List

1 – Invest in training

2 – Rebuild technical expertise lost to retirement and outsourcing

3 – Foster diverse viewpoints, consider minority views

4 – Use analytical tools

5 - Assess risk uniformly across all programs

Government Executive, April 15, 2004, *NASA's Next Step: First, Fix the Culture, Then Shoot the Moon*

Transformation Thoughts

- **Think nature of threat to get focus on capabilities.**
- **Only thing harder than getting new ideas in is getting old ideas out.**
- **Risk management is a key skill.**

Risk Management

Risk Management

"…part of everything we do. Risk management is the process of identifying and controlling hazards and making risk decisions to protect the force. It is applicable to any mission or environment, on or off duty."

Army Strategic Planning Guidance - 4 Dimensions of Risk

- **Operational Risk – ability to achieve military objectives in a near-term conflict or other contingency**
- **Future Challenges Risk – ability to invest in new capabilities and develop new operational concepts needed to dissuade or defeat mid-to long-term military challenges**
- **Force Management Risk – ability to recruit, retain, train, and equip sufficient numbers of quality personnel and sustain the readiness of the force while accomplishing its many operational tasks.**
- **Institutional Risk – ability to develop management practices and controls that use resources efficiently and promote the effective operations of the Defense establishment.**

4 Principles of Risk Management

- Manage risk in the planning stage
- Do not accept unnecessary risk
- Make risk decisions at the proper level
- Accept risk when benefits outweigh costs

5-Step Risk Management Process

1. **Identify Hazards to the force. Consider all aspects of current and future situations, environment, and know historical problem areas.**
2. **Assess Hazards to determine risk in terms of potential loss, cost, or mission degradation based upon probability an severity.**
3. **Develop Controls and Make Decisions that eliminate the hazard or reduce the risk.**
   - ✓ **Reassess hazards given the controls**
   - ✓ **Determine proper decision authority**

5-Step Risk Management Process [cont]

4. **Implement Controls that will eliminate the hazard or reduce the risk.**
5. **Supervise and Evaluate.**
   - ✓ **Enforce standards and controls.**
   - ✓ **Evaluate the effect of controls and adjust or update as necessary.**

1. Identify Hazards

- Hazard = any real or potential condition that can cause
  - Loss or damage to assets
  - Injury, illness, death of personnel
  - Mission degradation
  - Jeopardize achievement of an objective
- Sources of Hazards
  - Man – selection, performance, personal factors
  - Material – design, maintenance, logistics, tech data
  - Environment - operations
  - Management – standards, procedures, controls

Identifying Risks

- What could go wrong?
- How could we fail?
- What must go right for us to succeed?
- Where are we vulnerable?
- What resources (physical, information, people) do we need to protect?
- Do we have liquid assets or assets which could be used by others easily?
- How could someone steal from us?
- How could someone disrupt our operations?
- How do we know if we are achieving our objectives?
- On what information do we most rely?
- On what do we spend the most money?
- What decisions require the most judgment?
- What activities are most complex?
- What activities are regulated?
- What is our greatest legal exposure?

Types of Risk

Ownership Risks

- **External Threats – forces outside the control of the organization that can affect its business processes, and goals [customers, unions, regulation, economic and political forces, technology, physical and environment factors]**
- **Custodial Risks – owning and safeguarding assets [obsolescence, theft and damage from handling or storing]**
- **Hazards – loss or impairment from fire and other natural or man-made disasters and accidental loss**
- **Opportunity Costs – the cost of making less-than-optimum decisions about asset acquisition and disposition [paying too much, purchasing wrong asset]**

Process Risks

- **Hazards – loss or impairment from fire and other natural or man-made disasters and accidental loss**
- **Errors, Omissions, Delays – risks to processes arising from random differences in human or machine activity [poor judgment, inappropriate or outdated controls, malfunctions]**
- **Frauds – intentional misrepresentations of suppliers, employees, and customers**
- **Productivity Loss – poor design of the process or its control system [scheduling conflicts, inappropriate work rules, missing controls, lack of monitoring controls, underutilizing assets, goal conflicts]**

Behavioral Risks

- **Productivity Loss – poor design of the process or its control system [scheduling conflicts, inappropriate work rules, missing controls, lack of monitoring controls, underutilizing assets, goal conflicts]**
- **Dysfunctional Workplaces – risks to employees who work in a dysfunctional environment and risks to the organization because employees are working in such an environment [gender or racial harassment, excessive pressures to meet objectives without compensating relief valves, employee theft and sabotage, workplace injuries and violence, employee lawsuits]**
- **Opportunity Costs – the cost of making less-than-optimum decisions about asset acquisition and disposition [paying too much, purchasing wrong asset]**

10 Universal Business Risks

- Erroneous records and/or information
- Unacceptable accounting practices
- Business interruption
- Criticism or legal action
- High costs
- Unrealized or lost revenue
- Loss or destruction of assets
- Competitive disadvantage and/or public dissatisfaction
- Fraud or conflict of interest
- Inappropriate policy and/or decision making process

A “Working” Inventory of External Risks

Competition	Suppliers	Capacity
Regulatory	Political	Physical Disasters
Shareholder	Acquisition	Capital Availability
Environmental	Publicity	

A “Working” Inventory of Internal Risks

- Technology
  - Availability
  - Accuracy/Integrity
  - Confidentiality
  - Efficiency
- Operating
  - Customer Satisfaction
  - Compliance
  - Product Development
  - Brand Image
  - Third Party Providers
  - Business Performance Mgmt
- Strategic
  - Strategy
  - Resource Allocation
  - Cross Business Issues

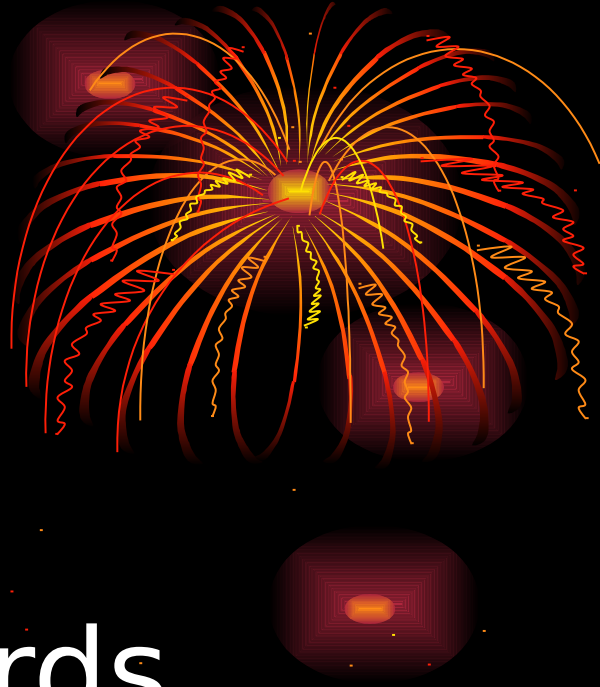
- Human Resources
  - Availability
  - Competency
  - Development
  - Safety
  - Integrity
  - Communication
  - Leadership
  - Empowerment
  - Rewards
- Financial/Regulatory/Mgmt Reporting
  - Existence
  - Completeness
  - Accuracy
  - Ownership
  - Disclosure
  - Valuation
  - Liquidity

Risk Identification Skills

Effect/Ultimate Consequence/Harm Done

Cause

Significance

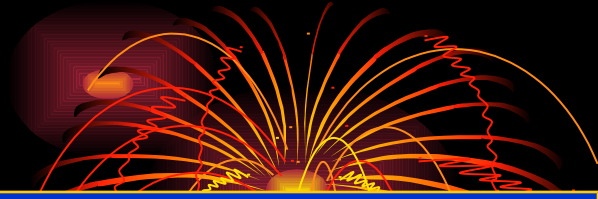


2. Assess Hazards

Risk Assessment Matrix

Likelihood →	Frequent	Likely	Occasional	Seldom	Unlikely
Impact ↓	A	B	C	D	E
Catastrophic I	Extremely High				
Critical II					
Marginal III	High				
Negligible IV	Medium	Low			

Assessing Risks



CATEGORY	LIKELIHOOD	SIGNIFICANCE
LOW	Unlikely risk Will occur	Probably will not materially impact attainment of objective if risk occurs
MEDIUM	Somewhat likely risk will occur	May impact attainment of objective if risk occurs
HIGH	Likely risk will occur	May significantly impact attainment of objective if risk occurs

3. Develop Controls and Make Decisions


Why We Need
Management or Internal
Controls?

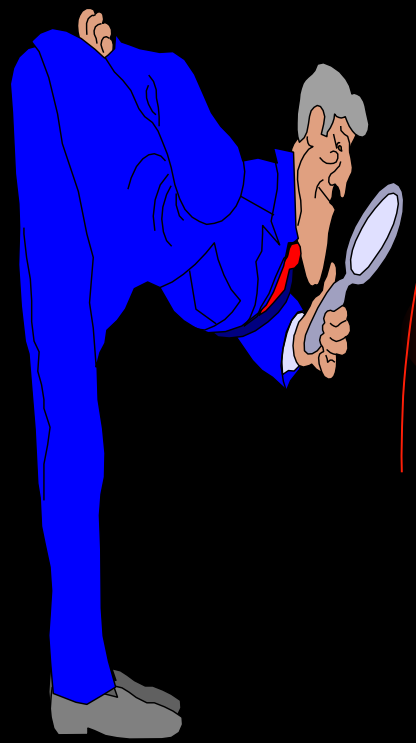
Controls

- Rules, procedures, regulations, directives, policies, techniques, and devices employed by managers to ensure that what should occur in their daily operations does occur on a continuing basis.
- Include such things as organizational structure, formally defined procedures, checks and balances, recurring reports and management reviews, supervisory monitoring, physical devices, and a broad array of measures taken by managers to provide reasonable assurance that their subordinates are performing as intended.

- ★*Risk*
- ★*Management Responsibilities*
- ★*It's the Law!*
- ★*Comptroller General Standards*
- ★*Army Regulation*

Risk

Competency Framework for Internal Auditing (CFIA) - Institute of Internal Auditors (IIA)



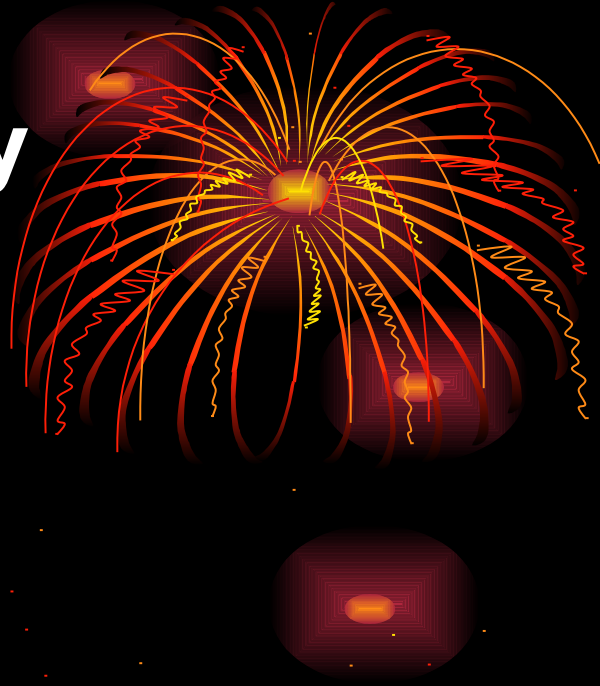
- **If there was no risk, there would be no need for controls.**
- **Controls only exist to manage risk.**
- **It is impossible to evaluate controls *effectively* without analyzing risk.**
- **The exposure to risk may be either positive - an opportunity, or negative - a threat.**

Fraud

- 15.4% of respondents stated the fraud was discovered with internal controls
- A strong system of internal controls was the most effective anti-fraud measure
- Relationship between fraud and internal controls
  - 46.2% said the victim lacked sufficient controls to prevent the fraud
  - 39.9% said the victim had sufficient controls, but they were ignored
  - 10.8% said the fraud could not have been prevented by standard internal controls
  - 3.1% said none of the above

Association of CFEs 2002 Report to the Nation on Occupational Fraud and Abuse

2003 KPMG Fraud Survey



- How was the fraud discovered?
  - Internal controls [77%]
  - Internal audit [65%]
  - Notification by employee [63%]
- What allowed the fraud to take place?
  - Collusion [63%]
  - Poor internal controls [39%]
  - Management override of controls [31%]
- What steps were taken to mitigate fraud?
  - Reviewed or strengthened internal controls [75%]
  - Instituted periodic compliance audits [44%]
  - Created an employee hotline [42%]

Management Responsibilities

- Inherent **Management** Responsibility
  - FM 101-5
    - A Good staff officer should possess and demonstrate: competence, initiative and judgment, creativity, flexibility, confidence, and loyalty. In addition, a good staff officer should be: a team player, an effective manager, an effective communicator.
    - An Effective Manager must be:
      - Able to effectively manage time and resources;
      - A good steward of resources that the country entrusts to his care;
      - Diligent in efforts to efficiently manage these resources, avoiding waste, destruction, and duplication of efforts.

- Inherent **Management** Responsibility
  - Management 101 – 5 functions of management
    - Planning
    - Organizing
    - Staffing
    - Directing
    - Controlling – the process of:
      - making certain that directed actions are carried out as planned in order to achieve some desired objective or goal
      - assessing controls

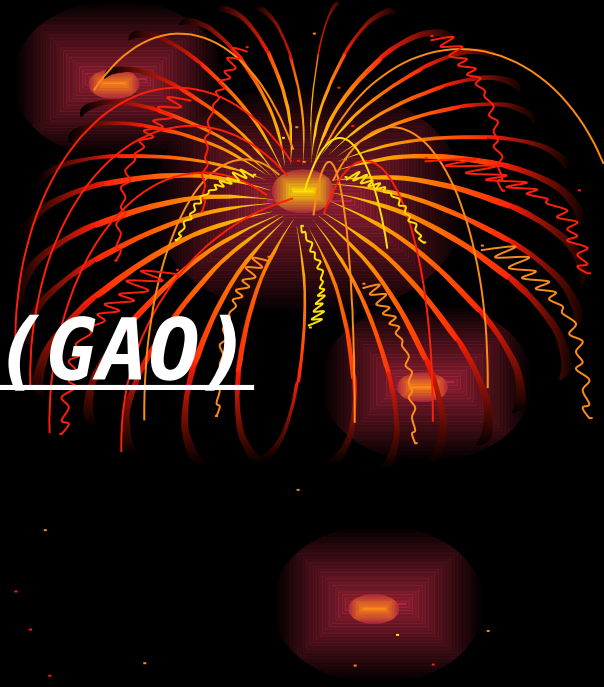
It’s the Law!

“This Administration is dedicated to ensuring that the resources entrusted to the federal government are well managed and wisely used. We owe that to the American people.”

President George W. Bush

Public Accountability

- Budget and Accounting Act of 1921
- Accounting and Auditing Act of 1950
- Federal Managers' Financial Integrity Act of 1982 (FMFIA)
- Chief Financial Officers Act (CFO) of 1990
- Government Performance and Results Act (GPRA) of 1993
- Government Management Reform Act (GMRA) of 1994
- Federal Financial Management Improvement Act (FFMIA) of 1996
- Sarbanes-Oxley Act of 2002



COMPTROLLER GENERAL'S (GAO) NEW [Nov 99] STANDARDS

- Control Environment
- Risk Assessment
- Control Activities
- Information and Communications
- Monitoring

10 - Turbulence from Change

“Conflicting priorities, downsizing, outsourcing, dependence on new and unproven systems or processes, de-emphasis on management controls and oversight, reorganization, sustained requirements growth despite resource constraints, and the need for frequent US military deployments are putting considerable strain on DOD’s human resources. This turbulent period is one of increased vulnerability to waste, fraud, and mismanagement. DOD can best mitigate that increased risk by paying careful attention to the need to improve, not eliminate, internal controls. One of the best ways to do so is to maintain a robust DOD audit and investigative effort.”

4. Implement Controls

5. Supervise and Evaluate

Why Risk Controls Fail

- Controls selected are inappropriate
- Operators don’t use controls
- Leaders don’t use or enforce controls
- Costs are more than anticipated
- Impede mission more than anticipated
- Get lost in the priority process
- Misunderstood

Enterprise Risk Management

Terms and Concepts

- **Business Risk**
  - The uncertainty of an event occurring that could have an impact on the achievement of objectives
  - The possibility that an event will occur and adversely affect the achievement of objectives
  - Risk is measured in terms of “likelihood” and “impact”
  - **Likelihood** = Probability that the event will occur
  - **Impact** = Consequences to the organization
  - Positive Risks = Opportunities

Uncertainty – inability to know in advance the exact likelihood or impact of future events

RM vs. ERM
The Essential Differences

Traditional Risk Management	Enterprise Risk Management
• Risk as individual hazards	• Risk in the context of business strategy
• Risk identification and assessment	• Risk "portfolio" development
• Focus on all risks	• Focus on critical risks
• Risk mitigation	• Risk optimization
• Risk limits	• Risk strategy
• Risks with no owners	• Defined risk responsibilities
• Haphazard risk quantification	• Monitoring and measurement
• Risk is not my responsibility	• Risk is everyone's responsibility

Source: KPMG & CFO Magazine

COSO's ERM Definition

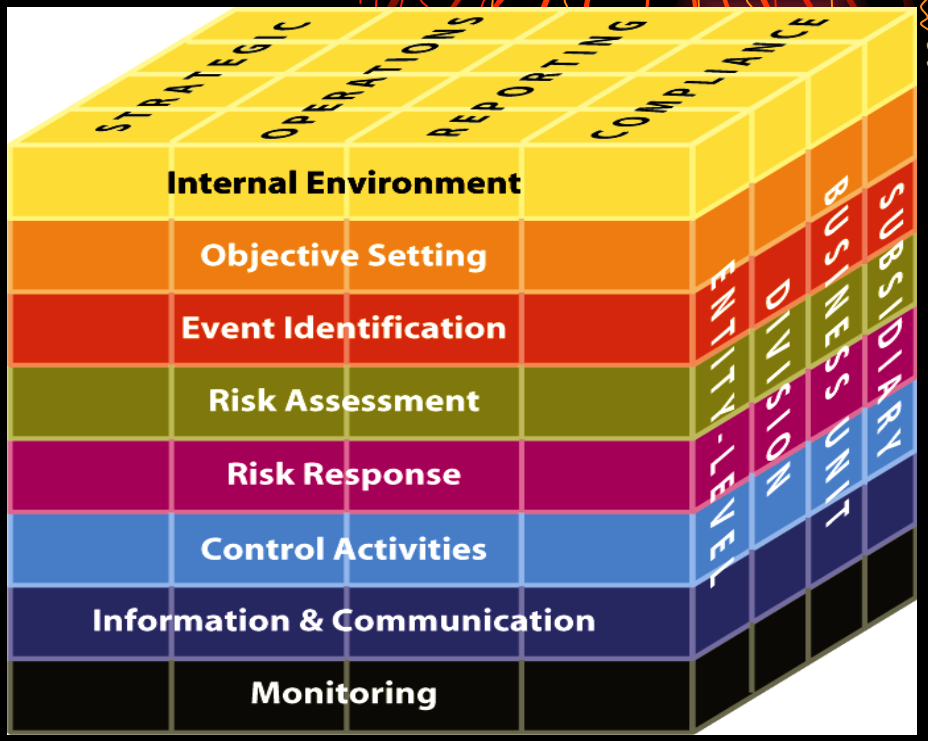
- Is a ***process*** – it's a means to an end, not an end in itself
- Is ***effected*** *by people* – it's not merely policies, surveys and forms, but involves people at every level of an organization
- Is ***applied*** *in strategy setting*
- Is ***applied*** *across the enterprise,* at every level and unit, and includes taking an entity-level portfolio view of risks
- Is designed to identify events potentially affecting the entity and manage risk within its ***risk appetite***
- Provides ***reasonable assurance*** to an entity's management and board
- Is geared to the ***achievement of objectives*** in one or more separate but overlapping categories.

COSO ERM Framework

Enterprise risk management is defined as follows:

A process effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of the following entity objectives:

- *Strategic*
- *Operational*
- *Reporting*
- *Compliance*



COSO identifies 8 components of ERM that need to be in place and integrated to ensure the achievement of each of the objectives.

ERM Objectives

The framework views entity objectives in the context of four categories:

- **Strategic –** relating to high-level goals, aligned with and supporting the entity's mission.
- **Operations** – relating to effective and efficient use of the entity's resources.
- **Reporting** – relating to the reliability of the entity's reporting.
- **Compliance** – relating to the entity's compliance with applicable laws and regulations.

ERM Components

Enterprise Risk Management consists of eight interrelated components that must be in place and working effectively.

- Internal Environment
- Objective Setting (process)
- Event Identification (process)
- Risk Assessment (process)
- Risk Response (process)
- Control Activities
- Information & Communication
- Monitoring

Internal Environment

The entity's internal environment is the foundation for all other components of enterprise risk management, providing discipline and structure. The internal environment influences how strategies and objectives are established, business activities are structured and risks are identified, assessed and acted upon.

- Risk Management Philosophy
- Risk Appetite
- Risk Culture
- Board of Directors
- Integrity and Ethical Values
- Commitment to Competence
- Management's Philosophy and Operating Style
- Organizational Structure
- Assignment of Authority and Responsibility
- Human Resource Policies and Practices

Risk Appetite

- Amount of risk an entity is willing to accept in pursuit of value
- Directly related to an entity's strategy
- Different strategies will expose an entity to different risks
- Guides resource allocation

Value – a measure of worth, utility, or importance

Risk Culture

- The set of shared attitudes, values, and practices that characterizes how an entity considers risk in its day-to-day activities

Objective Setting

Objective setting is a precondition to event identification, risk assessment, and risk response. There must first be objectives before management can identify risks to their achievement and take necessary actions to manage the risks.

- Strategic Objectives [high level goals]
- Operational Objectives [effectiveness and efficiency]
- Reporting Objectives [reliable, accurate, complete, intended purpose]
- Compliance Objectives
- Alignment of
  - Objectives
  - Risk Appetite
  - Risk Tolerance [acceptable levels of variation relative to achievement of objectives]

Event Identification

An event is an incident or occurrence emanating from internal or external sources that could affect implementation of strategy or achievement of objectives. Events may have positive or negative impacts, or both.

- Events
- Factors Influencing Strategy and Objectives [external and internal]
- Methodologies and Techniques
- Event Interdependencies
- Event Categories
- Risks and Opportunities

Methodologies and Techniques

- Event inventories – potential events common to organizations, or particular processes or activities
- Internal analysis
- Triggers – actual vs planned
- Facilitated workshops and interviews

Event Categories

Internal

- Infrastructure
- Personnel
- Process
- Technology

External

- Economic
- Business
- Technological
- Environment
- Political
- Social

Risk Assessment

Risk assessment allows an entity to consider the extent to which potential events might have an impact on achievement of objectives. Management should assess events from two perspectives (likelihood & impact) and normally uses a combination of qualitative and quantitative methods.

- Inherent [absence of any actions taken by mgmt] and Residual [after actions taken by mgmt] Risk
- Likelihood and Impact
- Methodologies and Techniques
- Correlation of Events

Risk Identification

- 3 Main Approaches
  - Exposure Analysis – identify risks that affect assets
    - Physical Financial
    - Human
    - Intangible, e.g., information, reputation
  - Environmental Analysis – identify risks that affect operations, management processes and controls
    - Current and future environment
    - Physical, economic, government regulation, competition, customers, technology
  - Threat Scenario – fraud, disasters, and security issues

Risk Response

Having assessed relevant risks, management determines how it will respond.

- Identify Risk Responses
- Evaluate Possible Risk Responses
  - Effect on likelihood and impact
  - Cost vs. benefits
- Select Responses
- Portfolio View
  - Entity-wide, directorate, division, branch, function

- **Common risk responses:**
  - **Avoid**: Redesign the process to avoid particular risks with the plan of reducing overall risk
  - **Diversify**: Spread the risk among numerous assets or processes to reduce the overall risk of loss or impairment
  - **Control**: Design activities to prevent, detect or contain adverse events or to promote positive outcomes
  - **Share**: Distribute a portion of the risk through a contract with another party, such as insurance
  - **Transfer**: Distribute all of the risk through a contract with another party, such as outsourcing
  - **Accept**: Allow minor risks to exist to avoid spending more on managing the risks than the potential harm

Control Activities

Control activities are the policies and procedures that help ensure that management's risk responses are carried out. Control activities occur throughout the organization, at all levels and in all functions.

- Integration with Risk Response
- Types of Control Activities
- General Controls
- Application Controls
- Entity Specific

Information & Communication

Pertinent information is identified, captured and communicated in a form and timeframe that enable people to carry out their responsibilities. Information systems use internally generated data, and information about external events, activities and conditions, providing information for managing enterprise risks and making informed decisions relative to objectives.

- Information
- Strategic and Integrated Systems
- Communication

"Risks not communicated are risks personally assumed."

Biggs C. Porter

Monitoring

Enterprise risk management is *monitored* – a process that assesses the presence and functioning of its components over time. This is accomplished through ongoing monitoring activities, separate evaluations or a combination of the two.

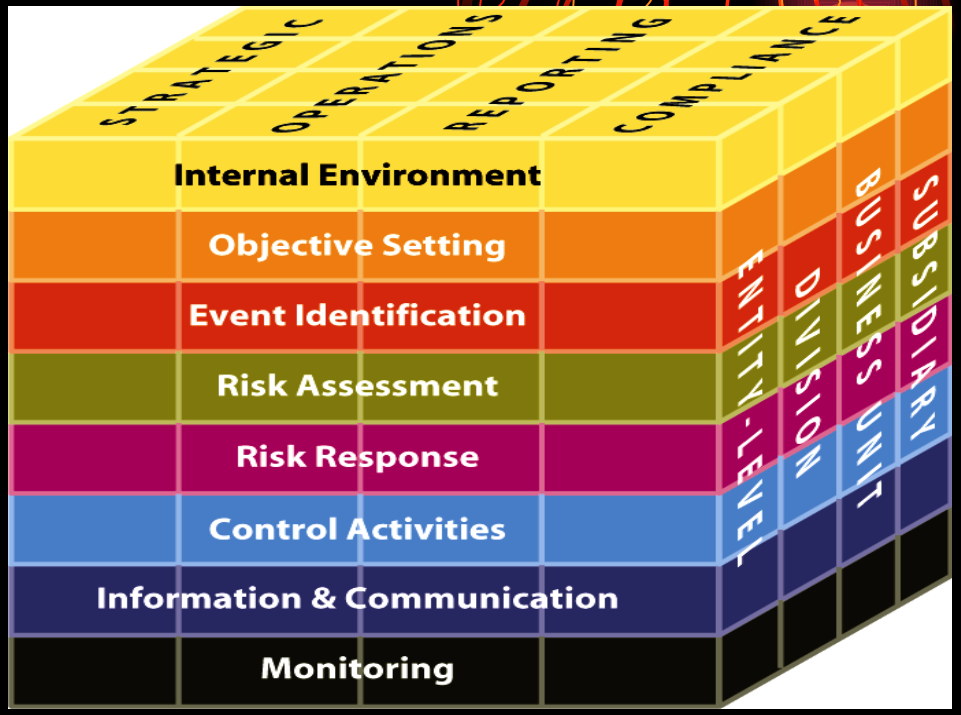
- Ongoing – “Built in”
- Separate Evaluations
- Reporting Deficiencies

COSO ERM Framework

Enterprise risk management is defined as follows:

A process effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of the following entity objectives:

- *Strategic*
- *Operational*
- *Reporting*
- *Compliance*



COSO identifies 8 components of ERM that need to be in place and integrated to ensure the achievement of each of the objectives.

ERM Benefits

- Improved Corporate Governance
  - Management accountability
  - Better Board reporting
  - Risk Champions (i.e. Chief Risk Office)
  - Better information flow
- Helps an organization attain its goals while avoiding pitfalls and surprises along the way
- Offers boards and management — regardless of the organization's size or scope — a commonly accepted model for discussing and evaluating the organization's risk management efforts

ERM Benefits

- **Enhances the organization's ability to:**
  - Align risk appetite and strategy
  - Link growth, risk, and return
  - Enhance risk response decisions
  - Minimize operational surprises and losses
  - Identify and manage cross-enterprise risks
  - Provide integrated responses to multiple risks
  - Seize opportunities
  - Rationalize resources
  - Deal effectively with potential future events that create uncertainty
  - Respond in a manner that reduces the likelihood of downside outcomes and increases the upside
  - Sustain value

ERM

- **Allows an organization to be "risk intelligent" by:**
  - **Systemically identifying potential exposures**
  - **Taking corrective actions early**
  - **Learning from these actions to better achieve objectives**

ERM Limitations

- Will help organizations get on track with their risk management processes. However, must acknowledge there's no substitution for integrity and an entity-wide understanding that controls are everybody's business.

- No guarantees. Management should be aware entity's goals might be affected by limitations inherent in their systems.
  - Human judgment in decision-making can be faulty
  - Breakdowns can occur because of human failures such as errors or mistakes
  - Controls can be circumvented by the collusion of two or more people
  - Management has the ability to override risk management processes, including risk response decisions and controls

- Comes at a Cost. Relative costs and benefits of risk responses need to be considered.

“A pint of sweat saves a gallon of blood.”

General George S. Patton

"There are risks and costs to a program of action. But they are far less than the long-range risks and costs of comfortable inaction."

John F. Kennedy

ERM

- **Endeavors fail if they lack:**
  - **Comprehensive risk-management architecture**
  - **Proper organization-supported climate**
  - **An in-house, trained champion**

Links to “Internal Control – Integrated Framework”

Framework Components

- Internal Environment
- **Objective Setting (process)**
- **Event Identification (process)**
- Risk Assessment (process)
- **Risk Response (process)**
- Control Activities
- Information & Communication
- Monitoring

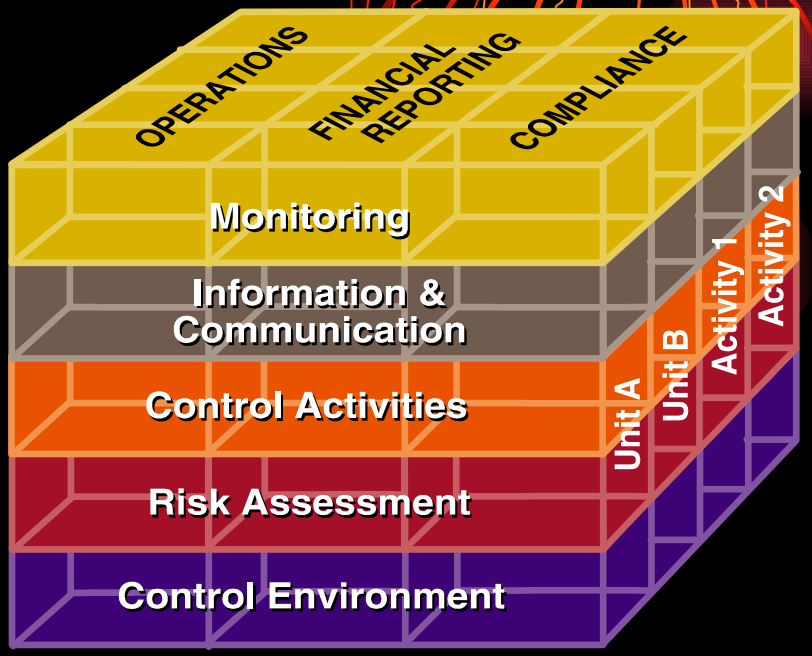
Links to "Internal Control – Integrated Framework"

- **Risk and control are inseparable like two sides of a coin:**
  - Risk: identified & assessed
  - Controls: managed & mitigated

COSO Internal Control Framework

Internal Control **is defined (in COSO and US auditing standards - AU 319) as a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:**

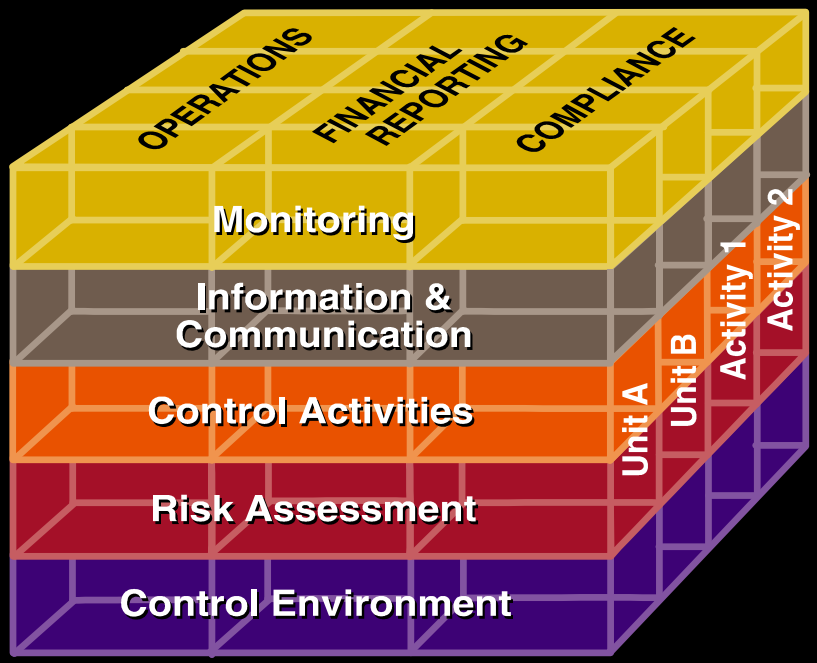
- *Effectiveness and efficiency of operations*
- *Reliability of financial reporting*
- *Compliance with applicable laws and regulations*



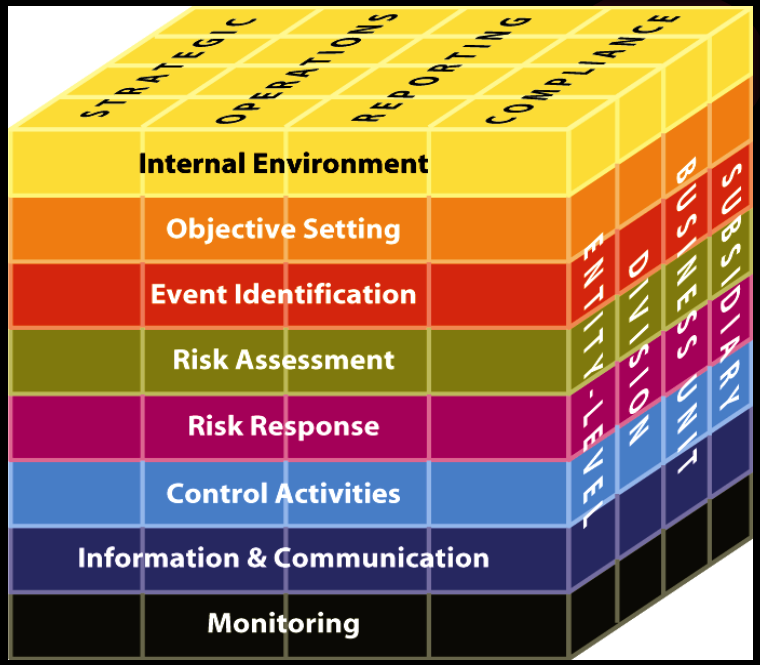
COSO identifies five components of internal control that need to be in place and integrated to ensure the achievement of each of the objectives.

Internal Controls & ERM

Internal Control
Integrated Framework



Enterprise Risk Management



Source: COSO

Keys to Implementation

- Start Small
  - Keep it discreet and manageable
  - Sources, processes, and scope of operations
- Doesn’t have to be complicated
  - Do need adequate resource commitments
  - Cross functional (horizontal) participation
- Implement in Phases
  - One size does not fit all
  - Integrate with culture and management styles
- Learn & Adapt
- Acknowledge that it comes at a price; be realistic

Keys to Implementation

- Senior Management Support
- ERM must be “built into” rather than “bolted onto” management’s planning and decision-making processes.
- Change Your Corporate Culture
- Consider creating a Chief Risk Officer
- Clearly Define roles & responsibilities
- Create an Enterprise Risk Committee
  - IR
  - G-8
  - Safety
  - G-2/G-6
  - IG
  - HR
  - SJA
  - “Line-of-business” leaders

Keys to Implementation

Questions Management and the Board Should Consider

- What is the organization's risk management philosophy?
- Is that philosophy clearly understood by all personnel?
- What are the relationships among ERM, performance, and value?
- How is ERM integrated within organizational initiatives?
- What is the desired risk culture of the organization and at what point has its risk appetite been set?
- What strategic objectives have been set for the organization and what strategies have been or will be implemented to achieve those objectives?
- What related operational objectives have been set to add and preserve value?
- What internal and external factors and events might positively or negatively impact the organization's ability to implement its strategies and achieve its objectives?
- What is the organization's level of risk tolerance?

Source: IIA's Tone At The Top (June 03)

Keys to Implementation

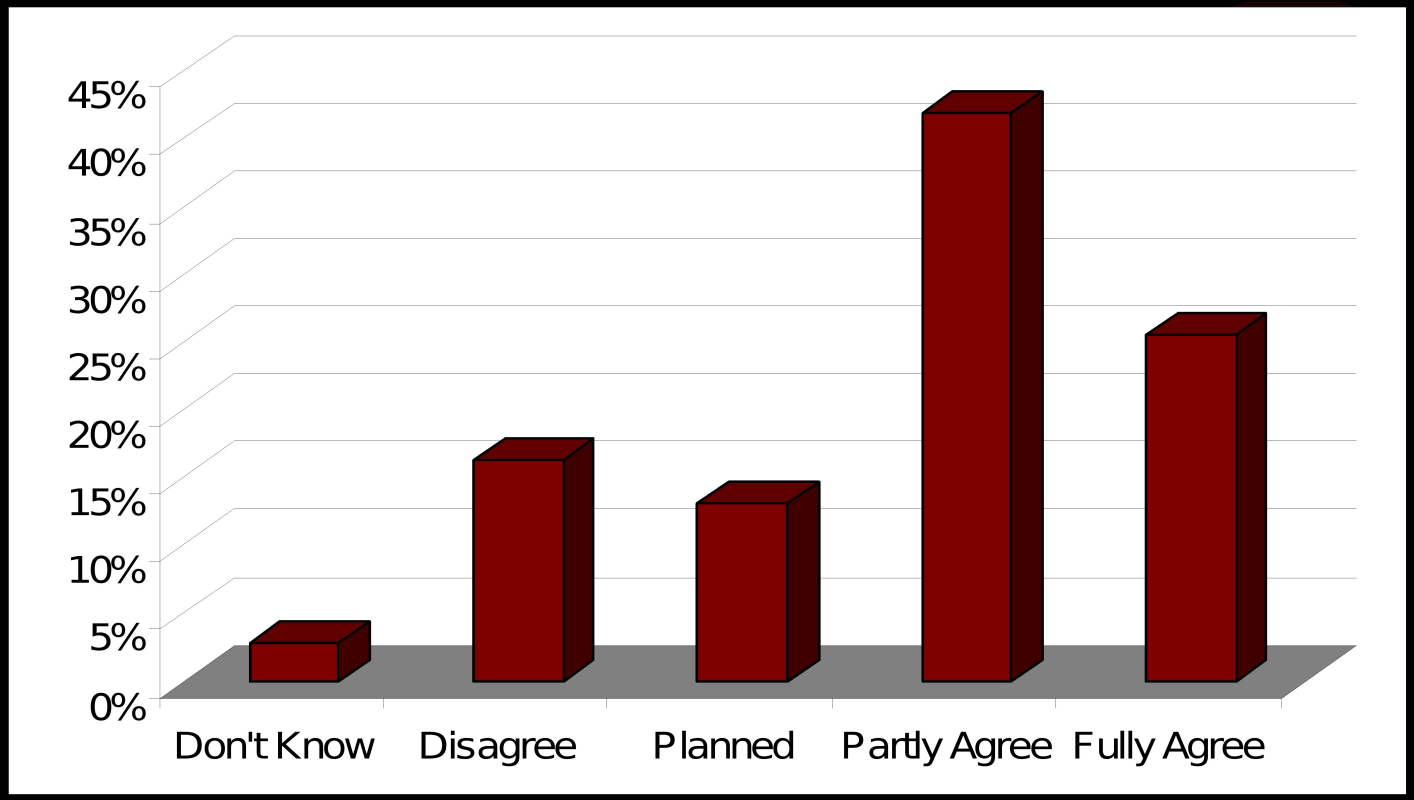
Questions Management and the Board Should Consider

- Is the chosen risk response appropriate for and in line with the risk tolerance level?
- Are appropriate control activities (i.e., approvals, authorizations, verifications, reconciliations, reviews of operating performance, security of assets, segregation of duties) in place at every level throughout the organization?
- Is communication effective — from the top down, across, and from the bottom up the organization?
- How effective is the process currently in place for exchanging information with external parties?
- What is the process for assessing the presence and performance quality of all eight ERM components over time?

Source: IIA's Tone At The Top (June 03)

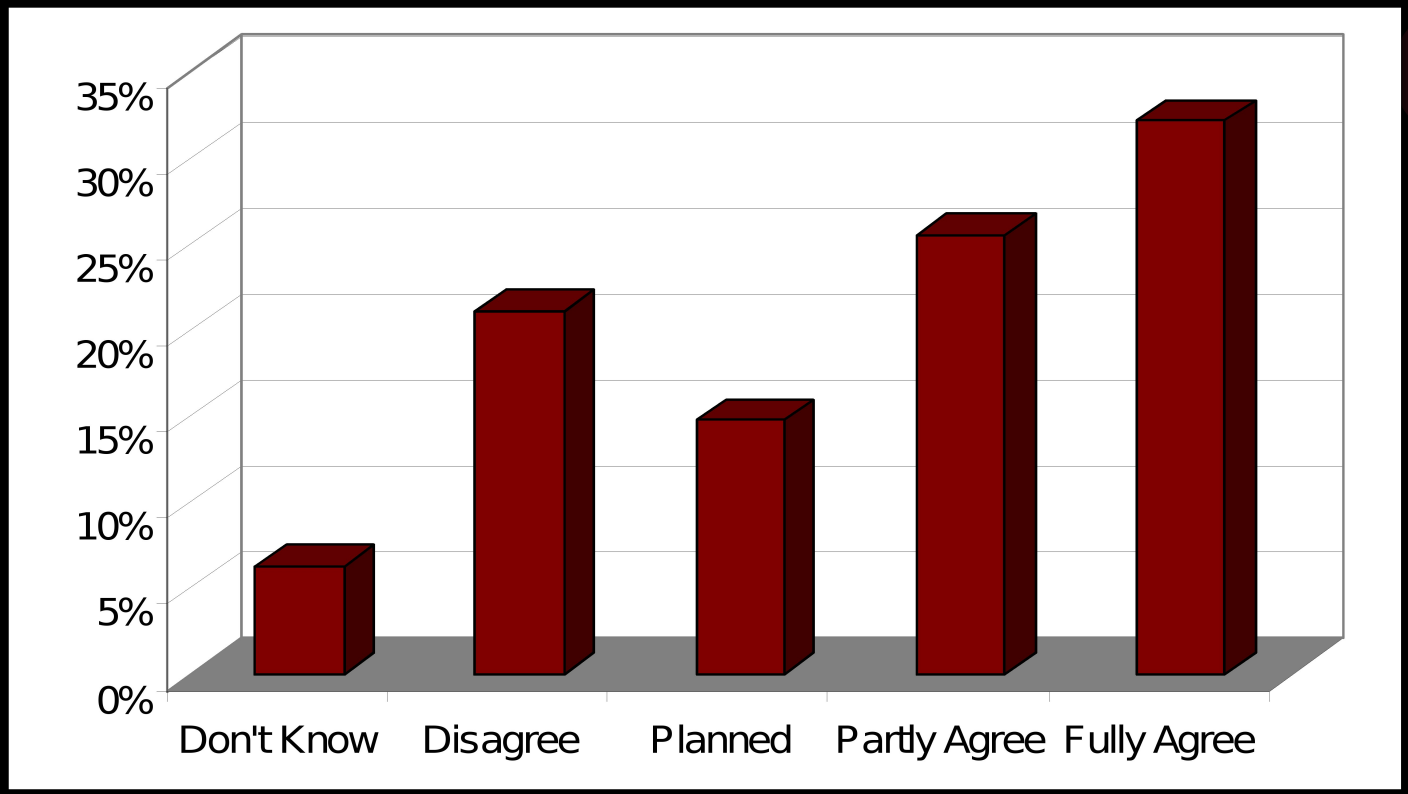
2003 G.A.I.N. Survey

1. The organization views risk management as a means of preserving and creating value



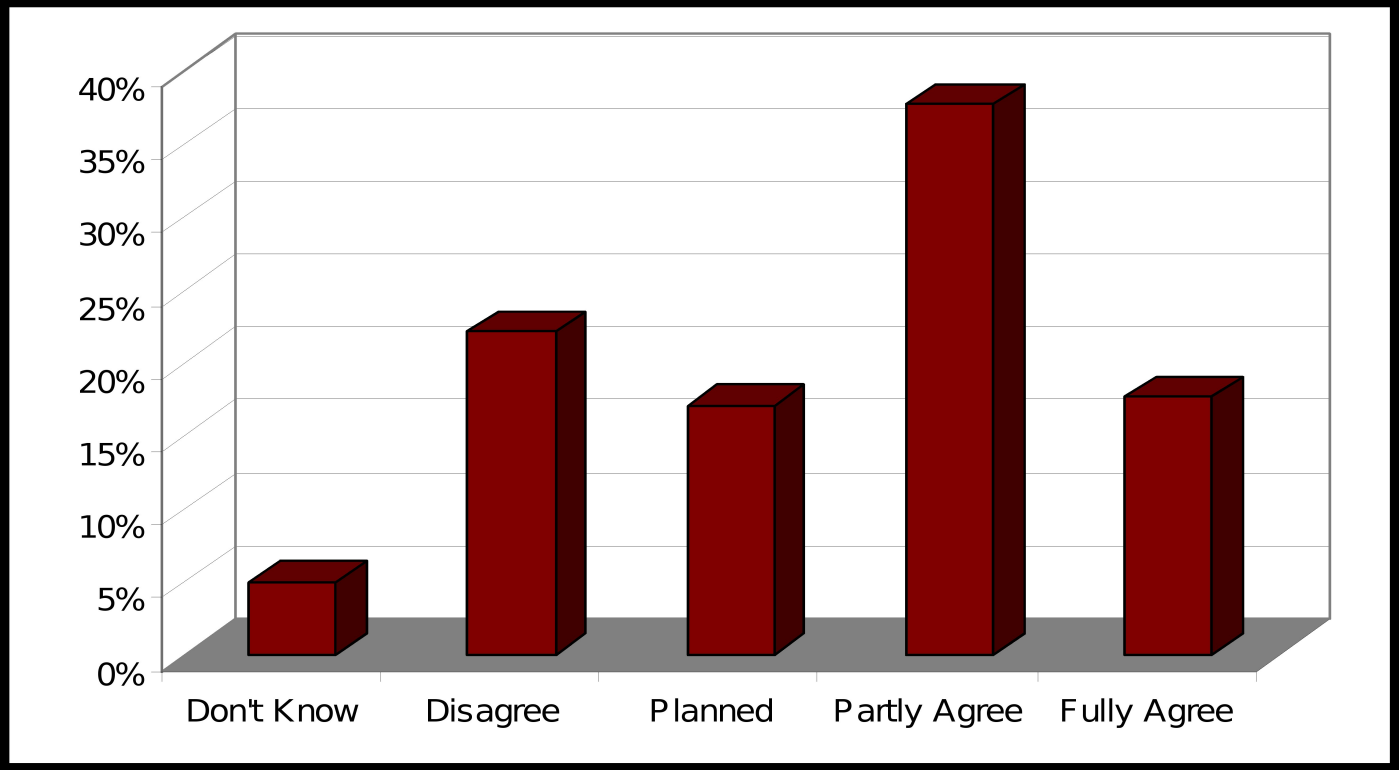
2003 G.A.I.N. Survey

2. The board considers risk management a regular part of its oversight agenda



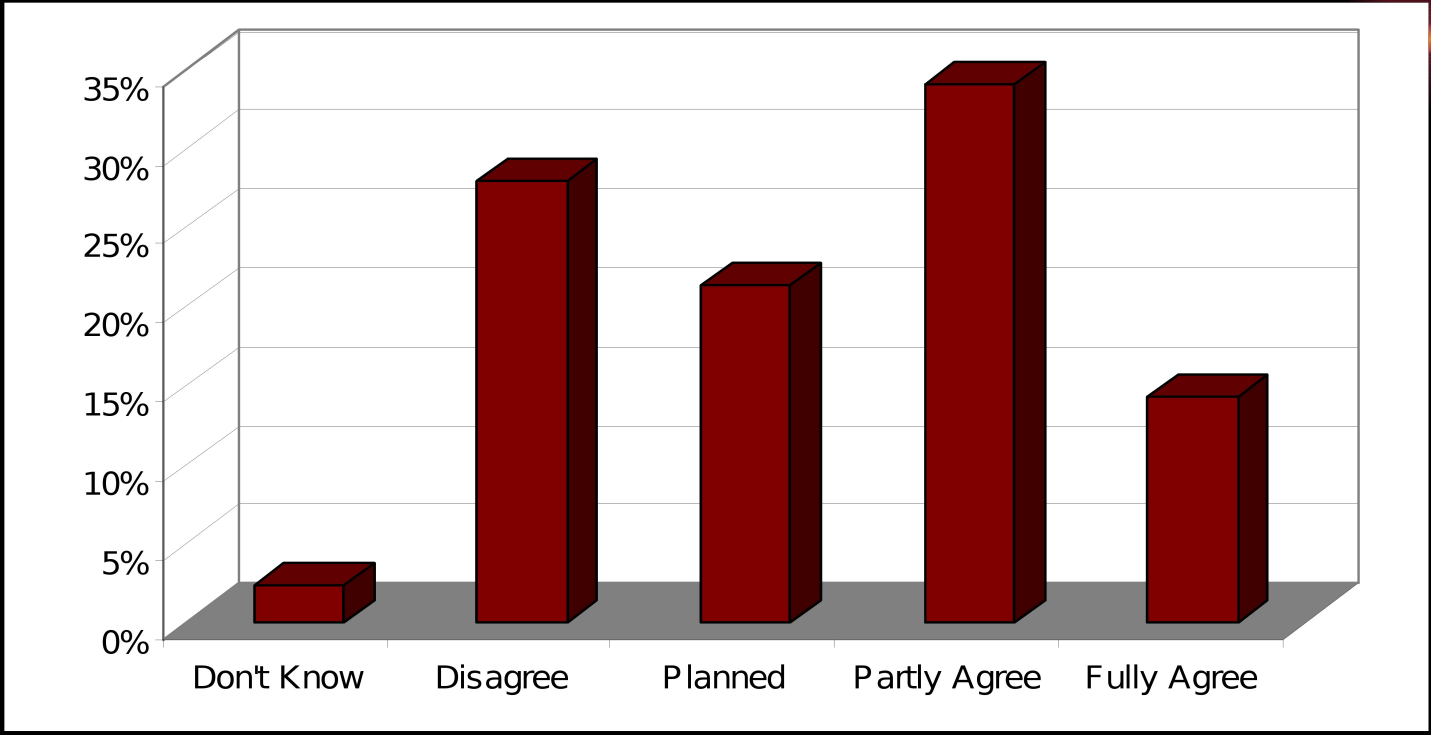
2003 G.A.I.N. Survey

3. The organizations attitude and approach to risk is clear and consistent with the level of risk (appetite) it is prepared to take



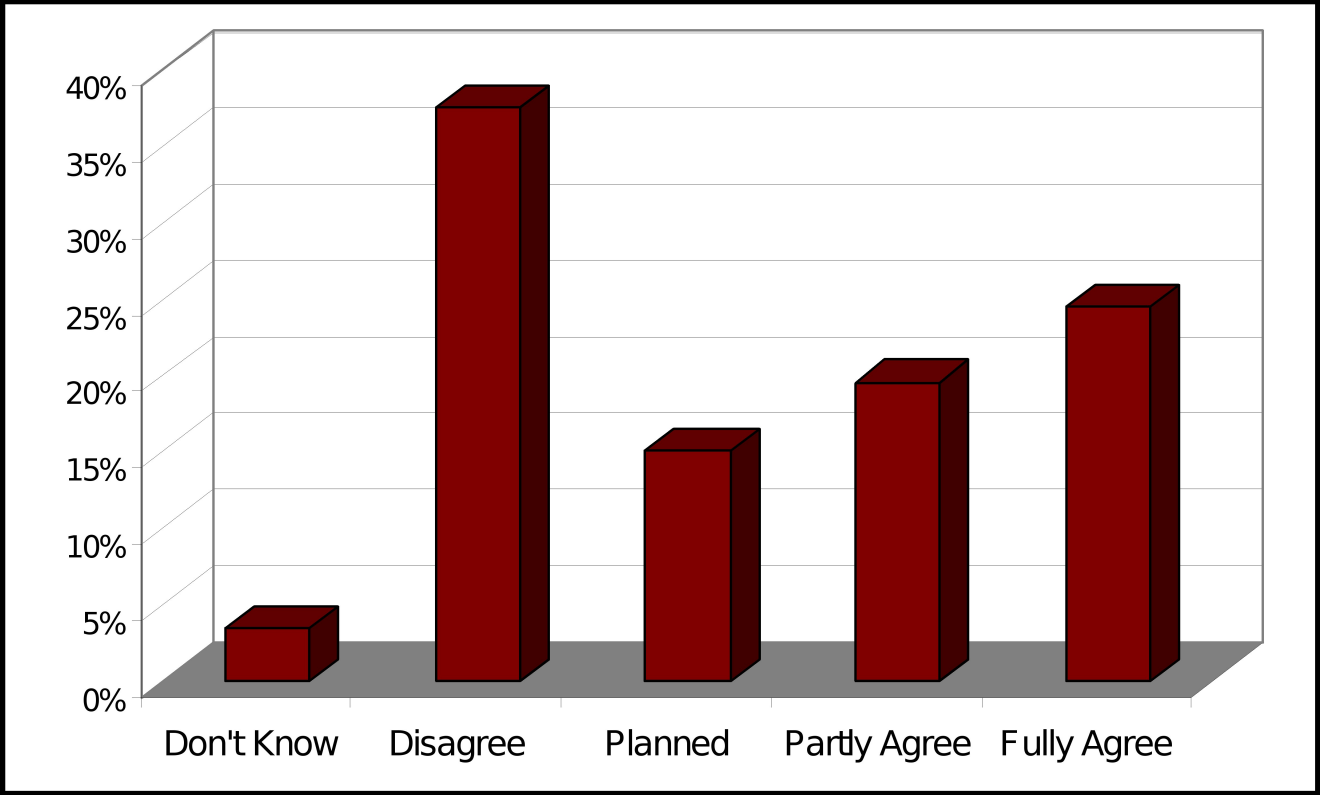
2003 G.A.I.N. Survey

4. Managers and personnel at all levels are involved in periodic review or planning exercises, which lead them to identify, source and quantify risks



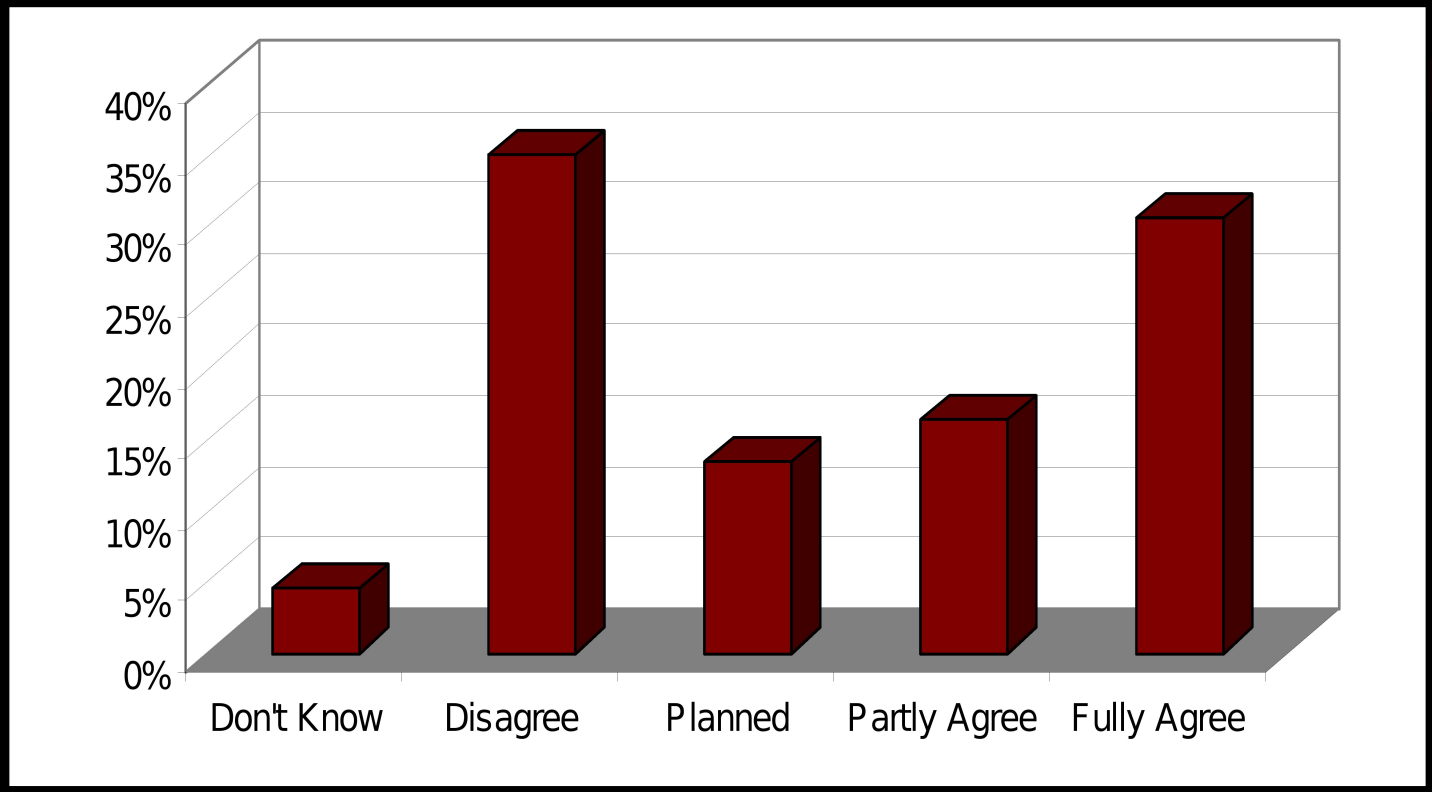
2003 G.A.I.N. Survey

5. There is a senior management committee that oversees risk management



2003 G.A.I.N. Survey

6. There is a senior executive responsible for risk management



Current Risk Management Tools

Institute of Internal Auditors [IIA]

IIA's revised definition of Internal Auditing (1999)

"Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and **improve the effectiveness of risk management**, control, and governance processes."

IIA Standard: 2110 – Risk Management

- **The internal audit activity should assist the organization by identifying and evaluating significant exposures to risk and contributing to the improvement of risk management and control systems.**
  - **2110.A1 - The internal audit activity should monitor and evaluate the effectiveness of the organization's risk management system.**
  - **2110.A2 - The internal audit activity should evaluate risk exposures relating to the organization's governance, operations, and information systems regarding the**
    - **Reliability and integrity of financial and operational information.**
    - **Effectiveness and efficiency of operations.**
    - **Safeguarding of assets.**
    - **Compliance with laws, regulations, and contracts.**

IIA Practice Advisories:

- **2100-3**: Internal Audit's Role in the Risk Management Process
- **2100-4**: Internal Audit's Role in Organizations Without a Risk Management Process
- **2110-1**: Assessing the Adequacy of Risk Management Processes

Risk Management and the Military Decision-Making Process (MDMP)

MDMP	Identify Hazards	Assess Hazards	Develop Controls, Make Risk Decisions	Implement Controls	Supervise and Evaluate
Mission Receipt	X				
Mission Analysis	X	X			
Develop COAs	X	X	X		
Compare COAs	X	X	X		
COA Approval			X	X	X

Generally Accepted Government Audit Standards (GAGAS)

GAGAS

- **In planning the audit, auditors should consider risks due to fraud [illegal act involving obtaining something of value through willful misrepresentation] that could significantly affect their audit objectives and the results of their audit.**
- **Auditors should exercise professional skepticism in assessing these risks to determine which factors or risks could significantly affect the results of their work if fraud has occurred or is likely to have occurred.**
- **Auditors should also be aware that assessing the risk of fraud is an ongoing process throughout the audit.**

GAGAS

- **In planning tests of compliance with significant laws and regulations, auditors should assess the risk that violations could occur.**
- **That risk may be affected by such factors as complexity or newness of the laws or regulations.**
- **The auditors' assessment of risk includes consideration of whether the entity has controls that are effective in preventing or detecting violations of laws or regulations.**

DoD IG Audit Manual

IG, DoD Internal Audit Manual, Jun 90

Chapter 5, Planning
Part II – Inventory of Auditable Entities

- Entities [activities, functions, programs, systems] subject to audit
- Priorities for audit coverage

- Adequacy of internal control systems
- Vulnerability to fraud, waste, abuse, mismanagement
- Newness or changes

IG, DoD Internal Audit Manual, Oct 99

Chapter 3, Planning

- Size and complexity of DoD make universal audit coverage on a cyclical basis generally impractical
- Audit planning process should focus on:
  - Regulatory and statutory requirements
  - Strategic management plan performance goals
  - Needs and concerns of management for oversight of key programs
  - Organization's mission
  - Balanced and adequate coverage of substantive operations, programs, and high-risk areas

Risk Management - According to IR

What it isn't and
What it is

Risk Management – According to IR -- What it isn't!

- **Safety's Risk Management Program – tactical and accident risks associated with operations and training**
  - **AR 385-10**
  - **FM 100-14**
  - **FM 100-5**
- **G-1's Risk Reduction Program – high-risk behaviors of Soldiers (deaths, accidents, injuries, suicide gestures and attempts, AWOLs, drug and alcohol offenses, and positive urinalysis)**

S.T.O.P.P.

- **Stop before you act, don't rush into a situation or mission without considering the risks against the benefits**
- **Think about what you are about to do, what is the right way to accomplish the task**
- **Observe the situation and surrounding environment. What are the risks? How can I reduce them?**
- **Plan to reduce the risks and decide how to best implement the plan.**
- **Proceed, supervise continuously and constantly look for ways to improve**

Risk Management – According to IR -- What it is!

- **Internal Review (IR)**
  - **AR 11-7, Internal Review and Audit Compliance Program**
  - **IR Guide**
- **Federal Managers' Financial Integrity Act (FMFIA) of 1982**
  - **AR 11-2, Management Control Process (MCP)**

The Army's Internal Review [IR] Program

AR 11-7

Broadening IR's Responsibilities

ASA(FM&C) 15 Sep 03 Memo announcing the Acting SecArmy's decision to not merge IR and USAAA

"the Army's need to strengthen the local management control process"

“Internal Audit Departments need to focus on adding real value by addressing the risks and issues that threaten their company’s ability to be successful in the cost reducing world we live in.”

IR Mission

To support Commanders with in-house, state-of- the-art, reliable, timely, professional reviews and consulting services that promote improved risk management and foster stewardship through best business practices

IR Guide, Chapter 1, Concept of Operations

Internal Review and Audit Compliance Manual, Aug 88

Chapter 9, Auditable Entity File

- Audit Planning Concepts:
  - Statutory and regulatory requirements
  - Adequacy of internal accounting and administrative control systems as indicated by vulnerability assessments and internal control reviews
  - Newness, changed conditions, or sensitivity of the organization, program, function
  - Current and potential dollar magnitude
  - Prior audit experience
  - Timelines, reliability, and scope of audits performed by others
  - Results of other evaluations, inspections, program reviews
  - Availability of audit resources

Internal Review and Audit Compliance Manual, Aug 88

Chapter 9, Auditable Entity File

- Serves as:
  - History of audit activity
  - Risk analysis of each auditable entity
  - Short and long-range planning too
  - Justification for manpower/resources
  - Audit Survey of past problems

Internal Review and Audit Compliance Manual, Aug 88

Chapter 9, Auditable Entity File

Risk Analysis

"Provides a formal and systemic basis for justifying the allocation of audit resources."

"Attempts to identify all the risks and then determine their severity."

President's Council on Integrity and Efficiency

Internal Review and Audit Compliance Manual, Aug 88

Chapter 9, Auditable Entity File
Risk Analysis

Risk Criteria

R1 Mission critical/morale impact
R2 Dollar value involved
R3 Potential for fraud, waste, abuse
R4 Past problem experience
R5 Potential embarrassment

Risk Ranking

1 = Low
2 = Medium low
3 = Medium
4 = Medium high
5 = High

Internal Review and Audit Compliance Manual, Aug 88

Chapter 9, Auditable Entity File

Risk Analysis

Sample Risk Assessment Matrix

Entity	R1	R2	R3	R4	R5	
Supply	5	5	5	4	4	23
Food Service	3	2	4	3	3	15
Warehouse	4	3	2	1	2	12
Mortuary	2	1	1	1	5	10

Risk Assessment/Management

- IR Director will assist commander in managing risk
- Not less than annually, formally report to the commander and staff the status of known risks within the command
- Normally this assessment done in concert with annual management control assessment and development of annual IR plan

AR 11-7 [draft]

Risk Assessment/Management

- Risks will be categorized based upon following criteria
  - Potential for adversely affecting mission accomplishment
  - Potential for loss of or minimize availability of resources (Fraud, Waste, Abuse)
  - Potential for adversely affecting employee or public safety
  - Potential violation of law, policy, or regulation
  - Potential for adverse publicity
  - Historical experience

AR 11-7 [draft]

Risk Assessment/Management

- High Risk areas identified will be appropriately addressed by the command through their system of oversight including but not limited to:
  - IR Reviews
  - External audits
  - IG Inspections/investigations
  - Organizational Inspection Programs
  - Safety Inspections
  - Force Protection Assessments
  - Management Control Process (MCP)

AR 11-7 [draft]

IR Director Responsibilities

- Ensure weaknesses identified through internal reviews and external audits are considered during preparation of the commander's annual assurance statement IAW AR 11-2.
- Review the organization's annual management control assurance statement and provide the commander an assessment of its thoroughness and validity.

AR 11-7 [draft]

Risk Assessment/Management

- Integral and ongoing responsibility of commanders
- Proactive and comprehensive IR Risk Management program
  - Identifies specific risks
  - Measures risks in terms of likelihood and consequences
  - Recommends corrective mitigating actions or controls
  - Performed as a member of the management team

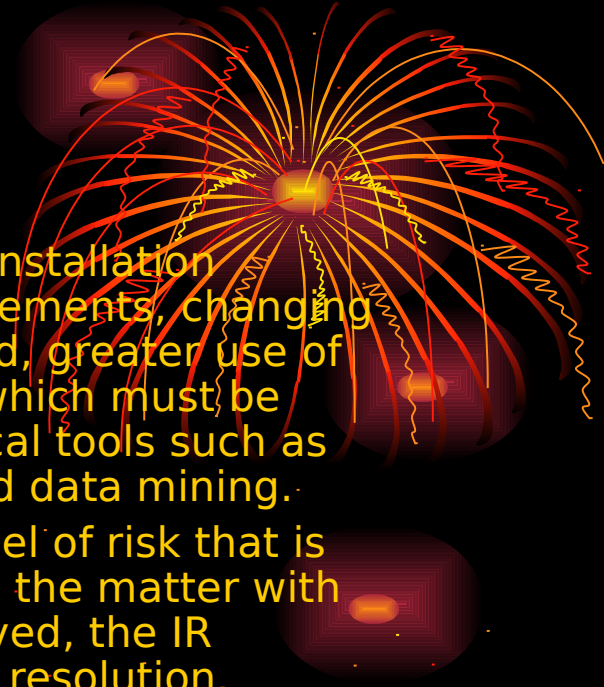
AR 11-7 [draft]

Risk Management

- Commanders have a statutory and regulatory resource stewardship responsibility to establish and maintain effective management controls.
- Corporate internal auditor being on-site is considered the in-house internal control expert assisting with: the assessment of risk; the design and implementation of mitigating controls; and testing of control compliance.
- IR fulfills this same important role for the Army commanders.
- Army resource stewardship is all about risk management.
- AR 11-2 sets forth the Army's management control process for assessing and then managing operating and fiscal risks.

IR Guide, Chapter 1, Concept of Operations

Risk Management



- With the Army's transformation initiative, restructuring of installation operations, emphasis to prepare auditable financial statements, changing business processes, military operations around the world, greater use of contractors, etc. new management risks are occurring which must be mitigated through controls that make use of technological tools such as system validation checks, system exception reports, and data mining.
- If the IR Director believes management has accepted a level of risk that is unacceptable to the organization, he/she should discuss the matter with management. If the decision regarding risk is not resolved, the IR Director should report the matter to the commander for resolution.
- Additional guidance on risk management is provided in Chapter 5.

IR Guide, Chapter 1, Concept of Operations

IR Planning Guidance Chapter 4, IR Guide

- Development of the IR Plan should be accomplished in concert with the command's MCP as well as the command's risk management program.
- Focus of the IR Plan will be directed high risk areas identified through the MCP or other command risk management initiatives.
- The "audit or oversight committee" will work with the IR Director and other oversight elements [IG, functional inspectors, safety and environmental, chartered management teams] to ensure high-risk areas are adequately covered.
- Request customer submit known or perceived risks or problem areas for potential IR assistance. Risks identified may or may not be the same as those reported to the audit/oversight committee or through the MCP.

Annual Internal Review (IR) Plan

- **Reviews scheduled for the FY/CY, prioritized and approved by the Commander**
- **Input from all customers/clients**
- **Customer/client performs risk assessment of their input**

Annual IR Plan – Risk Assessment

CRITERIA		LOW				HIGH
Mission/Readiness/Morale Impact	NA	1	2	3	4	5
Dollar Value Involved	NA	1	2	3	4	5
Potential for Fraud/Waste/Abuse	NA	1	2	3	4	5
Potential Violation of law, policy, or regulation	NA	1	2	3	4	5
Potential Adverse Impact on Employee/public safety	NA	1	2	3	4	5
Past Problem Experience	NA	1	2	3	4	5
Potential for Adverse Publicity	NA	1	2	3	4	5

The Army's Management Control Process [MCP]

AR 11-2

Army's Management Control Process (MCP)

- **The Army accepts a certain amount of risk by requiring assessable unit managers (AU concentrate on the adequacy o management controls, as specified in Comptroller General Standards, and key management controls, as specified by HQDA functional proponents**

The Internal Control Mystique

Myth	Fact
Starts with a strong set of policies and procedures	Starts with a strong control environment
Internal control is why we have auditors	Management owns internal control
A finance thing	Integral to every aspect of the business
Essentially negative, a list of “thou shalt nots”	Makes the right things happen the first time, and every time
A necessary evil. Take time away from core activities	Should be built into, not onto, business processes
If strong enough, no fraud	Provide reasonable, not absolute assurance

Elements of the Army's MCP

- ✓ **Key Management Controls**
- ✓ **Assessable Unit Managers (AUMs)**
- ✓ **Management Control Administrators (MCAs)**
- ✓ **5-year Plans**
- ✓ **Evaluations**
- ✓ **"Material" Weaknesses (MWs)**
- ✓ **Annual Statement of Assurance (ASA)**

AR 11-2

Key Management Controls

- **Absolutely essential to ensuring critical processes operate as intended and resources re safeguarded from fraud, waste, and abuse**
- **Fundamental criteria = severity of adverse impact should the control fail, or fail to be used**
- **Those whose failure would “break” or seriously impair the system**

5-Year Plans

- **Plan for conducting required management control evaluations**
- **Identifies**
  - **What is to be evaluated**
  - **Who will conduct the evaluation**
  - **When it will be evaluated based upon**

Risk

Evaluations

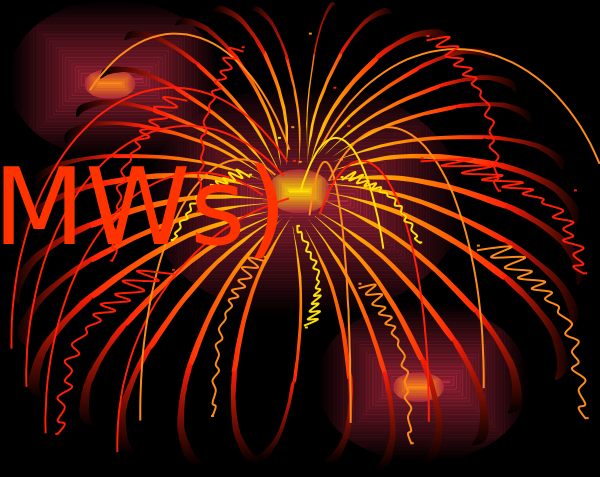
- **Detailed, systemic, and comprehensive examination of key management controls to determine whether they:**
  - **Are in place**
  - **Being used as intended**
  - **Are effective in achieving their purpose**
- **Involve testing and supporting documentation**

Control Weaknesses

- Needed controls are not prescribed (in rules, policies, or procedures) and actual practices do not include needed controls
- Needed controls are not prescribed but actual practices include needed controls
- Prescribed controls are inadequate, incomplete, or ineffective and actual practices do not include adequate controls
- Prescribed controls are inadequate, incomplete, or ineffective but actual practices include adequate controls

- Prescribed controls are adequate, but are not followed
- Control objective is not stated
- Stated control objective is not adequate

Material Weaknesses (MWs)



- **Two Conditions must exist:**
  - **It must involve a weakness in management controls**
  - **It must warrant the attention of the next level of command either because the next level must:**
    - **Take action or**
    - **Be aware of the problem**
- **Subjective management judgment by AUMs**

MWs

A “significant” management control weakness is one

that needs to be reported to a higher level of command or another command for either their resolution/action or awareness

What is Significant?

If the answer is YES to any of the below factors, it likely constitutes a MW [more Yes answers more likely a MW]

- ✓ Actual or potential loss of assets
- ✓ Actual or potential frequency of loss
- ✓ Sensitivity of resources involved
- ✓ Magnitude of funds, property, or other resources involved
- ✓ Impaired fulfillment of essential mission
- ✓ Current or probable media interest (adverse publicity)
- ✓ Congressional, DOD, or DA interest

What is Significant?

If the answer is YES to any of the below factors, it likely constitutes a MW [more Yes answers more likely a MW]

- ✓ **Unreliable information causing unsound management decisions**
- ✓ **Diminished credibility or reputation of management**
- ✓ **Statutory or regulatory violations**
- ✓ **Impact on information security**
- ✓ **Safety (injury or life-threatening situation)**
- ✓ **Public deprived of a needed service**

Issues and Concerns

- Management Control Weaknesses not considered material or significant
- Any thing that impacts or may impact mission, readiness, or any of the factors for determining significance
- Resource shortfalls

Future Risk Management Tools

Keys to Implementation

ERM Readiness Quiz

Are you up to the challenge of helping your organization implement ERM? The following self-assessment quiz may help you decide whether your audit shop is ready to take on this role.

Consider each of the four audit department attributes on the five-point scales shown and rate your department accordingly. After completing the four boxes, add your numbers and compare your total to the grading guide.

	1	2	3	4	5
AUDIT APPROACH	Controls-based				Risk-based
AUDIT ROLE	"Gotcha" (policeman)				Consultative
VIEWPOINT	Toward the past				Toward the future
SKILL SET	Traditional accounting/ auditing tools				ERM competency facilitator

SCORING

APPROACH	+	ROLE	+	VIEWPOINT	+	SKILLS	=	YOUR SCORE

GRADING GUIDE	
15-20	Ready for ERM participation
10-14	Further preparation needed
4-9	Considerable change required for ERM readiness

Source: *Internal Auditor* (Aug 03)

Internal Audit's Role

- *"Internal Controls - Integrated Framework"* sat on the shelves for nearly 10 years. Why will this be any different?
- Internal Auditors must play a proactive role and facilitate risk management in their organizations.
- Participator & Evaluator
- Promote and evaluate risk management, ethics, corporate governance
- Incorporate with SOX efforts

Internal Audit's Role

- Championing the risk management process
- Providing advice to management on embedding risk management processes into the business
- Evaluating the risk management process
- Lead the coordination of the risk management process

Top 10 ways for Internal Audit to get involve
Corporate Governance

1. Become involved in corporate compliance programs.
2. Assist in the development, implementation, and monitoring of governance principles.
3. Get involved in the disclosure control process of the chief executive officer/chief financial officer certification process.
4. Increase internal control awareness in your organization focusing on internal audit department core competencies.
5. Improve the internal audit department's relationship with the organization's external auditor.

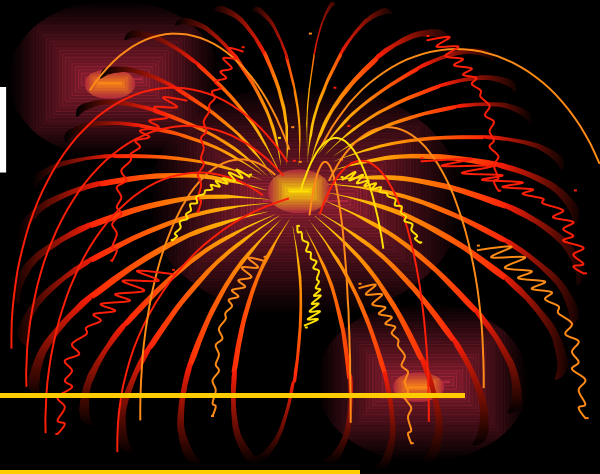
Source: IIA's CSA Sentinel (Oct 03)

Top 10 ways for Internal Audit to get involve
Corporate Governance

6. Enhance the internal audit department's relationship with the audit committee and ensure proper reporting and independence.
7. **Get involved with the company's enterprise risk management program.**
8. Increase ethical behavior oversight.
9. Determine the internal auditor's role in the internal control assessment requirements.
10. Develop a method to ensure the proper balance of internal audit department work.

Source: IIA's CSA Sentinel (Oct 03)

Implementing ERM



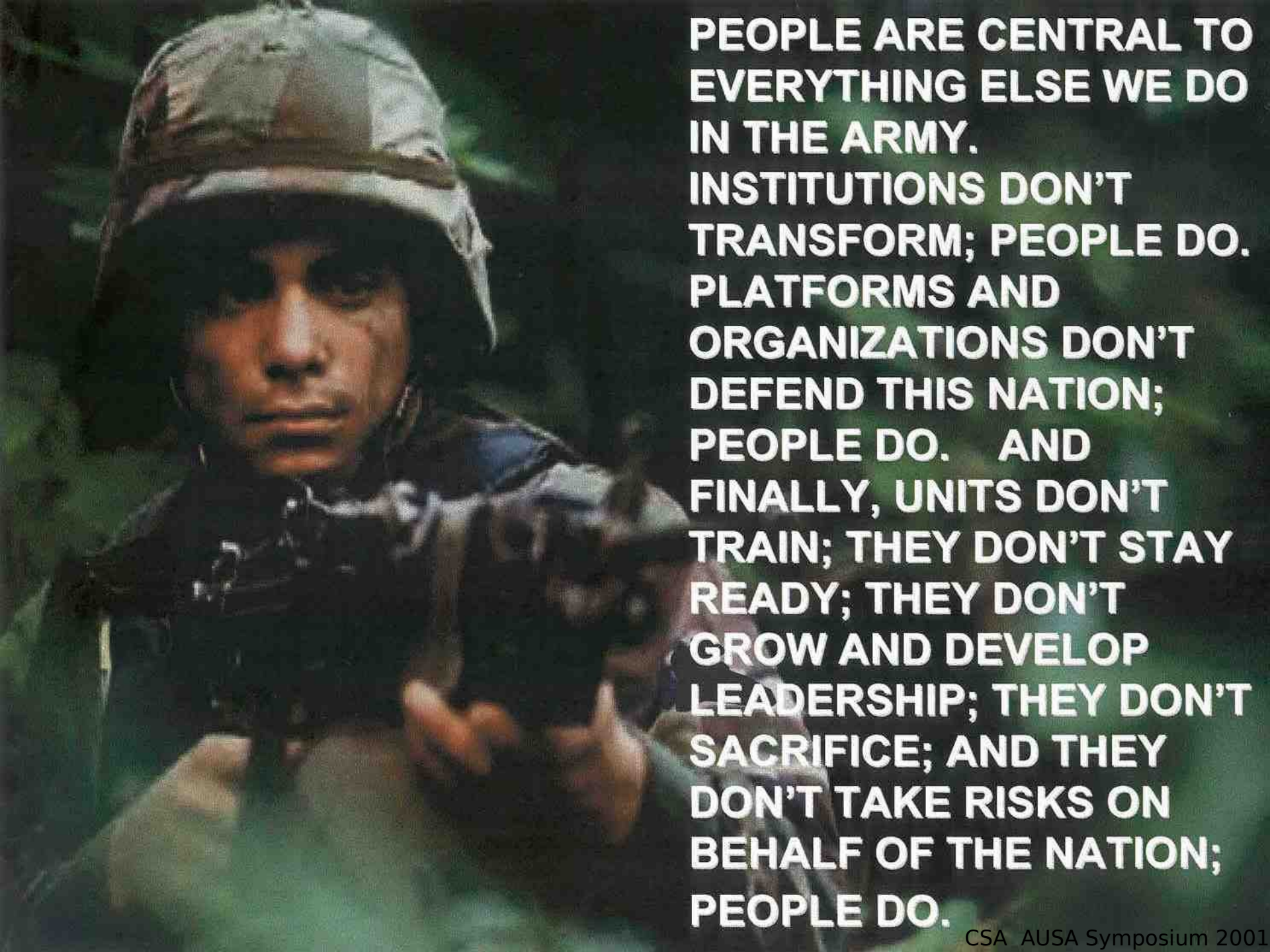
Function:_____

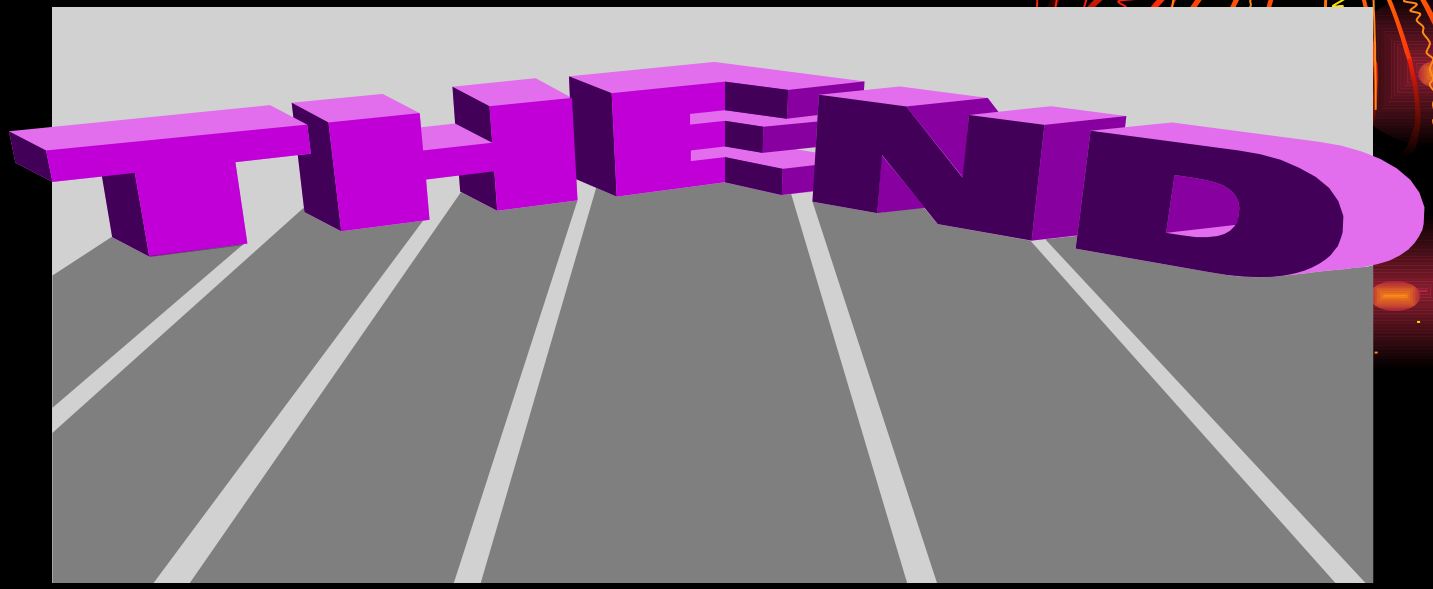
Mission/Objectives:_____

What Could Go Wrong	Likelihood H	M	L		Impact H	M	L
1.							
2.							
3.							

H=High, M=Medium, L=Low

Process Action Team on “Broadening IR’s Responsibilities” Update


PEOPLE ARE CENTRAL TO EVERYTHING ELSE WE DO IN THE ARMY.
INSTITUTIONS DON'T TRANSFORM; PEOPLE DO.
PLATFORMS AND ORGANIZATIONS DON'T DEFEND THIS NATION; PEOPLE DO. AND FINALLY, UNITS DON'T TRAIN; THEY DON'T STAY READY; THEY DON'T GROW AND DEVELOP LEADERSHIP; THEY DON'T SACRIFICE; AND THEY DON'T TAKE RISKS ON BEHALF OF THE NATION; PEOPLE DO.



DIRECTOR, IR, U.S. ARMY RESERVE